

ENTERED

August 10, 2017

David J. Bradley, Clerk

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

MANTISSA CORPORATION,

Plaintiff,

V.

ONDOT SYSTEMS, INC.; LONE STAR
NATIONAL BANK; and LONE STAR
NATIONAL BANCSHARES-TEXAS, INC.,

Defendants.

CASE NO. 4:15-CV-1133

MEMORANDUM OPINION

Plaintiff Mantissa Corporation (“Mantissa”) brings this suit for patent infringement under 35 U.S.C. § 271 against Defendants Ondot Systems, Inc., Lone Star National Bank, and Lone Star National Bancshares-Texas, Inc. (collectively, “Defendants”). Now pending before the Court are Defendants’ “Motion for Judgment on the Pleadings and Renewed Motion for Judicial Notice,” ECF No. 80, and Defendants’ “Motion to Strike Plaintiff’s Unauthorized Reply and Declaration,” ECF No. 107.

I. BACKGROUND

A. The Patents-in-Suit

This case concerns U.S. Patent Nos. 7,779,456 (“the ’456 Patent”) and 8,353,027 (“the ’027 Patent”). The ’456 Patent was filed on April 27, 2005 and issued on August 17, 2010. The application for the ’027 Patent was a continuation of the patent application that issued as the ’456 Patent. The ’027 Patent was filed on July 26, 2010 and issued on January 8, 2013.

Both of the patents-in-suit are titled “System and Method for Enhanced Protection and Control Over the Use of Identity” and relate to a “method of protecting use of an entity’s

identity.” In particular, the patents purport to “provide[] protection of the identity of an entity by placing limitations or conditions on its use, and whereby the entity’s use-enabling identification information is not fully needed to authorize a transaction.” ECF No. 38-1 at 1:9–14.

B. The Asserted Claims

Mantissa alleges that Defendants “have committed, and continue to commit, direct acts of infringement of the ’456 Patent and the ’027 Patent by making, using, offering to sell and selling products, systems and services embodying the patented invention.” ECF No. 38 ¶ 15. Mantissa asserts infringement of fifty-two total claims: claims 1–7 and 11–29 of the ’456 Patent and claims 1–3 and 7–29 of the ’027 Patent (the “asserted claims”). ECF No. 38 at ¶¶ 21, 29.

Of the fifty-two asserted claims, nine are independent claims: claims 1, 2, 4, 5, 11, and 15 of the ’456 Patent, and claims 1, 7, and 11 of the ’027 Patent. The remaining forty-three asserted claims are dependent claims.

The text of claims 1, 5, 11, and 15 of the ’456 Patent is as follows:

1. A method of protecting use of an entity’s identity, the method being executed on electronic computer hardware in combination with software, the method comprising:
 - setting a status of the identity to a first state, the first state defining a scope of permitted use of the identity;
 - changing, in advance of an intended use of the identity, the status to a second state defining a scope of permitted use of the identity that is different from the first state;
 - requesting use of the identity after said changing; and
 - returning, after said requesting, the state back to the first state;
 - wherein the first state is a default state, and said returning occurs in response to completion of a use of the identity;
 - wherein said requesting comprises transmitting, from a user of said identity to a service provider which maintains the state, a request for authorization to use the identity, where information in the request is insufficient to authorize the use of the identity;
 - wherein said setting, changing, requesting and returning are executed on electronic computer hardware in combination with software.

ECF No. 38-1 at 15:8–28.

5. A method of protecting use of an entity's identity, the method being executed on electronic computer hardware in combination with software, the method comprising:

- attempting to use an identity at a source;
 - forwarding first information relating to said use to a user affiliated with the source location;
 - forwarding second information from the user to a service provider, the second information being different from the first information;
 - determining, by the service provider, whether said use of the identity is consistent with at least one pre-registered condition; and
 - sending, from the service provider to the user, a decision based on the determining;
- wherein the second information is insufficient in and of itself to authorize any related use of the identity;
- wherein the at least one pre-registered condition defines at least one circumstance under which the identity can be used.

ECF No. 38-1 at 16:4–22.

11. A method of protecting use of an entity's identity, the method being executed on electronic computer hardware in combination with software, the method comprising:

- establishing, by the user, a set of desired identification information parameters;
 - sending, from the user to a service provider, the set;
 - obtaining, by the service provider from the entity, information from the entity consistent with the set, the information including at least one pre-determined condition;
 - storing the information provided by said obtaining; and
 - using, by the service provider, at least some of the at least one pre-determined condition and at least some of the information provided in said obtaining to respond to a request by the user to authorize a use of the identity of the entity;
- wherein the user does not have direct access to the information provided by the entity and subject to said storing;
- wherein the at least one pre-registered condition defines at least one circumstance under which the identity can be used.

ECF No. 38-1 at 16:42–61.

15. A method of protecting use of an entity's identity, the method being executed on electronic computer hardware in combination with software, the method comprising:

storing, at a service provider, data representing first identification information of an entity, and at least one criteria capable of limiting the use of the identity;

receiving, at a service provider, a request to determine whether the use of an entity's identity by a party is authorized for a requested application, the request including second identification information;

comparing at least some of the first identification information with at least some of the second identification information;

first determining whether the request is consistent with at least one pre-determined condition;

second determining, based at least partially on a result of said comparing and said first determining, whether the use of the identity by the identity-use-source is authorized for a particular application; and

responding from the service provider to the identity-use source consistent with the result of said determining;

wherein the at least one pre-registered condition defines at least one circumstance under which the identity can be used.

ECF No. 38-1 at 17:4–28.

The text of claims 1, 7, and 11 of the '027 Patent is as follows:

1. A method of protecting use of an entity's identity when the entity attempts to use the identity, the method being executed on electronic computer hardware in combination with software, the method comprising:

receiving, at a service provider, information regarding the attempted use of the entity's identity, the information being insufficient in and of itself to execute the attempted use of the identity;

determining, at the service provider, whether the attempted use of the entity's identity is consistent with at least one pre-registered condition;

sending, from the service provider, a decision based on the determining;

wherein the at least one pre-registered condition defines at least one circumstance under which the identity can be used; and

wherein the service provider lacks sufficient data to execute the attempted use of the identity.

ECF No. 38-2 at 15:18–35.

7. A method of protecting use of an entity's identity, the method being executed on electronic computer hardware in combination with software, the method comprising:

receiving, at a service provider, a set of desired identification information parameters from a user;

obtaining, at the service provider, information from the entity consistent with the set, the information including at least one pre-determined condition defined by the entity;

storing, at the service provider, the information provided by the obtaining;
receiving, at the service provider, a request to authorize use of the entity's identity;
using, at the service provider, at least some of the at least one pre-determined condition and at least some of the information provided in the obtaining to respond to the request to authorize a use of the identity of the entity;
wherein third parties other than the service provider, the entity and authorized agents do not have direct access to the information from the entity from the obtaining and subject to the storing;
wherein the at least one pre-registered condition defines at least one circumstance under which the identity can be used.

ECF No. 38-2 at 15:53–16:9.

11. A method of protecting use of an entity's identity, the method being executed on electronic computer hardware in combination with software, the method comprising:

storing, at a service provider, data representing first identification information of an entity, and at least one entity defined criteria capable of limiting the use of the identity;
receiving, at a service provider, a request to determine whether the use of an entity's identity by a party is authorized for a requested application, the request including second identification information;
comparing at least some of the first identification information with at least some of the second identification information;
first determining whether the request is consistent with at least one pre-determined condition;
second determining, based at least partially on a result of the comparing and the first determining, whether received request represents an authorized use of the entity's identity for a particular application; and
transmitting information consistent with the result of the determining;
wherein the at least one pre-registered condition defines at least one circumstance under which the identity can be used; and
wherein the service provider lacks sufficient information to execute the attempted use of the identity.

ECF No. 38-2 at 16:20–46.

The Court has construed the following claim terms:

- “identity” means “identification information.”
- “entity” means “the owner of the identity.”
- “user” means “requester of use of entity's identity.”

- “source” means “a person or thing from which the inquiry comes into being or is derived or obtained.”
- “identity-use-source” means “a party/point at which use of the entity’s identity is attempted.”
- “service provider” means “that which addresses requests for identity use.”
- the phrases “information . . . is insufficient to authorize the use of the identity”/ “the second information is insufficient in and of itself to authorize any related use of the identity”/ “the information being insufficient in and of itself to execute the attempted use of the identity” mean “the information is sufficient for the service provider to determine whether the intended use of the identity is proper, but not enough to authorize/execute the use/related use/attempted use of the identity.”
- “the service provider lacks sufficient data/information to execute the attempted use of the identity” means “the service provider has enough information to determine whether the attempted use of the identity is proper, but not enough to execute the attempted use of the identity.”
- “scope of permitted use” means “set of conditions under which the identity may or may not be used.”

Mantissa Corp. v. Ondot Sys., Inc., No. 4:15-CV-1133, 2017 WL 1373771, at *3–12 (S.D. Tex. Jan. 13, 2017), *adopted*, No. 4:15-CV-01133, 2017 WL 1383884 (S.D. Tex. Apr. 13, 2017) (Ellison, J.).

C. Procedural History

Mantissa filed its original complaint in this case on April 29, 2015. Defendants subsequently filed a Rule 12(b)(6) motion to dismiss. ECF No. 20. On April 14, 2016, United States District Judge Keith P. Ellison granted that motion on grounds that “the patents are invalid because they are drawn to an abstract idea.” ECF No. 35 at 36.

On May 3, 2016, Mantissa filed its first amended complaint, which remains the live pleading. ECF No. 38. Defendants subsequently moved to dismiss the amended complaint under Rule 12(b)(6), again on grounds that the patents-in-suit are directed to a patent-ineligible abstract idea. ECF No. 45. Defendants also filed a motion requesting the court to take judicial notice of a 1995 American Bar Association Guide to Wills & Estates, subtitled “Everything You Need to

Know About Wills, Trusts, Estates, and Taxes.” ECF No. 46. On August 11, 2016, Judge Ellison denied the motion to dismiss, concluding that the issue of patent eligibility should not be decided until claim construction had occurred. ECF No. 58. Judge Ellison also denied the motion for judicial notice as moot. *Id.*

Judge Ellison then referred the case to this Court to conduct a claim construction hearing in accordance with *Markman v. Westview Instruments, Inc.*, 517 U.S. 370 (1996). ECF No. 68. The Court held the *Markman* hearing and issued a report and recommendation, which Judge Ellison adopted on April 13, 2017. ECF Nos. 76, 94.

While objections to the report and recommendation were pending before Judge Ellison, Defendants filed a combined motion for judgment on the pleadings and renewed motion for judicial notice—one of the motions now before the Court. ECF No. 80. On May 12, 2017, Judge Ellison transferred the case to this Court to conduct all further proceedings in accordance with 28 U.S.C. § 636(c). ECF No. 99. After reviewing the then-pending motions, the Court convened a telephone status conference on May 24, 2017. ECF No. 100. The Court informed the parties of its decision to convert the Rule 12(c) motion for judgment on the pleadings into a Rule 56 motion for summary judgment and set deadlines for the parties to file additional briefing. The Court held a hearing on Defendants’ converted summary judgment motion on August 7, 2017.

II. LEGAL STANDARD AND APPLICABLE SUBSTANTIVE LAW

A. Summary Judgment Standard

Summary judgment is appropriate when “there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law.” FED. R. CIV. P. 56(a). An issue of fact is “material” if its resolution in favor of one party might affect the outcome of the lawsuit under governing law. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986); *Sossamon v.*

Lone Star State of Tex., 560 F.3d 316, 326 (5th Cir. 2009) (internal quotation marks and citation omitted). A dispute about a material fact is “genuine” when “the evidence is such that a reasonable jury could return a verdict for the nonmoving party.” *Anderson*, 477 U.S. at 248; *Quality InfusionCare, Inc. v. Health Care Serv. Corp.*, 628 F.3d 725, 728 (5th Cir. 2010) (internal quotation marks and citation omitted).

The party moving for summary judgment bears the initial burden of “identifying those portions of the record it believes demonstrate the absence of a genuine issue of material fact.” *Triple Tee Golf, Inc. v. Nike, Inc.*, 485 F.3d 253, 261 (5th Cir. 2007) (citing *Celotex Corp. v. Catrett*, 477 U.S. 317, 322–25 (1986)). If the movant meets its initial burden, the nonmoving party must then identify specific evidence in the record demonstrating that there is a material fact issue and articulate how that evidence supports its case. *Baranowski v. Hart*, 486 F.3d 112, 119 (5th Cir. 2007). “This burden will not be satisfied by ‘some metaphysical doubt as to the material facts, by conclusory allegations, by unsubstantiated assertions, or by only a scintilla of evidence.’” *Boudreaux v. Swift Transp. Co.*, 402 F.3d 536, 540 (5th Cir. 2005) (quoting *Little v. Liquid Air Corp.*, 37 F.3d 1069, 1075 (5th Cir. 1994) (en banc)).

On a motion for summary judgment, a court must view the evidence and draw all reasonable inferences in the light most favorable to the nonmoving party. *Connors v. Graves*, 538 F.3d 373, 376 (5th Cir. 2008); *Reaves Brokerage Co. v. Sunbelt Fruit & Vegetable Co.*, 336 F.3d 410, 412 (5th Cir. 2003). A court may consider any evidence in “the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any.” *Kee v. City of Rowlett*, 247 F.3d 206, 210 (5th Cir. 2001) (internal quotation marks omitted) (quoting *Celotex Corp.*, 477 U.S. at 322). However, “[w]hen evidence exists in the summary judgment record but the nonmovant fails even to refer to it in the response to the motion for summary

judgment, that evidence is not properly before the district court.” *Malacara v. Garber*, 353 F.3d 393, 405 (5th Cir. 2003). “Rule 56 does not impose upon the district court a duty to sift through the record in search of evidence to support a party’s opposition to summary judgment.” *Id.* (internal quotation marks and citations omitted). A court may also consider any materials properly subject to judicial notice. *MacMillan Bloedel Ltd. v. Flintkote Co.*, 760 F.2d 580, 587 (5th Cir. 1985); *see also* FED. R. EVID. 201.

B. Patent Subject-Matter Eligibility

Defendants in this case move for summary judgment on grounds that the asserted claims of the patents-in-suit are directed to an “abstract idea” and are therefore ineligible for protection under the Patent Act.

Section 101 of the Patent Act provides that “[w]hoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.” 35 U.S.C. § 101.¹ The Supreme Court has long held that § 101 “‘contains an important implicit exception: Laws of nature, natural phenomena, and abstract ideas are not patentable.’” *Alice Corp. Pty. v. CLS Bank Int’l*, 134 S. Ct. 2347, 2354 (2014) (quoting *Ass’n for Molecular Pathology v. Myriad Genetics, Inc.*, 133 S. Ct. 2107, 2116 (2013)); *accord* *Diamond v. Diehr*, 450 U.S. 175, 185 (1981) (collecting cases). At the same time, the Supreme Court has cautioned that courts must “tread carefully in construing this exclusionary principle lest it swallow all of patent law.” *Alice*, 134 S. Ct. at 2354. “At some level, ‘all inventions . . . embody, use, reflect, rest upon, or apply laws of nature, natural phenomena, or abstract ideas.’” *Id.* (quoting *Mayo*,

¹ A “process” is statutorily defined as a “process, art or method, and includes a new use of a known process, machine manufacture, composition of matter, or material.” 35 U.S.C. § 100(b). The parties do not dispute that the methods described in the asserted claims otherwise qualify as a “process” under § 101.

566 U.S. at 71). “Thus, an invention is not rendered ineligible for patent simply because it involves an abstract concept.” *Id.* Rather, so long as an invention applies an abstract concept “to a new and useful end,” it remains patent-eligible under § 101. *Id.* (internal quotation marks omitted) (quoting *Gottschalk v. Benson*, 409 U.S. 63, 67 (1972)).

Whether a patent’s subject matter is eligible for protection under § 101 is a question of law. *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1369 (Fed. Cir. 2011). “The § 101 inquiry ‘*may* contain underlying factual issues.’” *Mortg. Grader, Inc. v. First Choice Loan Servs. Inc.*, 811 F.3d 1314, 1325 (Fed. Cir. 2016) (quoting *Accenture Glob. Servs., GmbH v. Guidewire Software, Inc.*, 728 F.3d 1336, 1341 (Fed. Cir. 2013)) (emphasis added in *Mortg. Grader*). “But it is also possible, as numerous cases have recognized, that a § 101 analysis may sometimes be undertaken without resolving fact issues. In such circumstances, the § 101 inquiry may appropriately be resolved on a motion for summary judgment.” *Id.* (internal citation omitted).

“There is no clear mandate from the Supreme Court or the Federal Circuit” regarding “what burden of proof is applicable to a § 101 challenge.” *Network Apparel Grp., LP v. Airwave Networks Inc.*, 154 F. Supp. 3d 467, 474 (W.D. Tex. 2015), *adopted*, No. 6:15-CV-00134, 2016 WL 4718428 (W.D. Tex. Mar. 30, 2016), *aff’d*, No. 2016-1943, 2017 WL 957238 (Fed. Cir. Mar. 13, 2017). Lower courts are divided on that question, with some requiring that a party asserting a § 101 challenge prove ineligibility by “clear and convincing evidence” and others applying a less demanding “preponderance of the evidence” standard. *See Network Apparel Grp.*, 154 F. Supp. 3d at 475 & n.2 (collecting cases). The Court need not resolve this issue in the present case. Even if “clear and convincing evidence” is the proper standard, it applies only “to questions of fact and not to questions of law.” *See Microsoft Corp. v. i4i Ltd. P’ship*, 564

U.S. 91, 114 (2011) (Breyer, J., concurring). As explained below, there are no material fact issues in this case, and Defendants are entitled to summary judgment as a matter of law.

III. DISCUSSION

The Supreme Court has set forth a two-step analysis, now widely referred to as the *Alice* framework, for “distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts.” *Alice*, 134 S. Ct. at 2355. The Court’s task in this case is to determine whether Defendants are entitled to summary judgment by applying *Alice* to the asserted claims of the patents-in-suit.

A. *Alice* Step One: The Asserted Claims Are Directed to an Abstract Idea

At Step One of *Alice*, the Court must determine whether the asserted claims are “directed to” a patent-ineligible abstract idea. *See Alice*, 134 S. Ct. at 2355. More specifically, the Court must consider the asserted claims “in their entirety” and “in light of the specification[s]” in order to ascertain whether their “character as a whole” is “directed to excluded subject matter.” *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335 (Fed. Cir. 2016); *Internet Patents Corp. v. Active Network, Inc.*, 790 F.3d 1343, 1346 (Fed. Cir. 2015).

1. The “Character as a Whole” of the Asserted Claims

Determining the asserted claims’ “character as a whole” entails “identify[ing] and defin[ing] whatever fundamental concept appears wrapped up in the claim[s].” *Accenture Glob. Servs., GmbH v. Guidewire Software, Inc.*, 728 F.3d 1336, 1341 (Fed. Cir. 2013) (internal quotation marks omitted). Other cases have described the claims’ “character as a whole” as their “focus” or “basic thrust.” *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016); *Bascom Glob. Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1348 (Fed. Cir. 2016). The Court must be “careful not to express the claim’s fundamental concept at an unduly

‘high level of abstraction . . . untethered from the language of the claims,’ but rather at a level consonant with the level of generality or abstraction expressed in the claims themselves.” *X One, Inc. v. Uber Techs., Inc.*, No. 16-CV-06050-LHK, 2017 WL 878381, at *8 (N.D. Cal. Mar. 6, 2017) (quoting *Enfish*, 822 F.3d at 1336).

a. The Independent Claims

The Court looks first to the nine asserted independent claims, beginning with claim 1 of the ’456 Patent. As its opening words state, claim 1 is aimed at “protecting use of an entity’s identity.” ECF No. 38-1 at 15:1. Reading claim 1 in its entirety reveals that the key role in accomplishing that end falls to the “service provider,” which must determine whether a given use of the identity is permitted. *See Mantissa Corp.*, 2017 WL 1373771, at *3–5 (adopting Mantissa’s proposed construction of the term “service provider” as meaning “that which addresses requests for identity use”). Claim 1 further specifies that the service provider makes its determination based on two inputs: (i) the “scope of permitted use,” and (ii) “information in the request [for authorization, which] is insufficient to authorize the use of the identity.” The Court construed “scope of permitted use” to mean “set of conditions under which the identity may or may not be used.” *Mantissa Corp.*, 2017 WL 1373771, at *10–12 (adopting Mantissa’s proposed construction). It also construed the phrase “information . . . is insufficient to authorize the use of the identity” as “the information is sufficient for the service provider to determine whether the intended use of the identity is proper, but not enough to authorize the use of the identity.” *Id.* at *6–9 (adopting Mantissa’s proposed construction). Thus, the service provider makes its determination based on: (i) a set of conditions defining when the identity may or may not be used; and (ii) information that is, in itself, insufficient to permit use of the identity. The specification confirms that the service provider, and, more specifically, the information on which

the service provider bases its determination with respect to a given use of an identity, forms the “focus” or “basic thrust” of the claim. Claims 2 and 4 of the ’456 Patent are identical to claim 1 with respect to the central role of the service provider.

Reading the other six independent claims in their entirety reveals that they share the same “fundamental concept” as claim 1 of the ’456 Patent. In all of these claims, the service provider performs the crucial role of deciding whether a particular use of an identity is permitted based on essentially the same two inputs used in claim 1 of the ’456 Patent. To be sure, there are differences in terminology, but those distinctions do not change the focus of those claims. Claims 1, 2, and 4 of the ’456 Patent refer to the set of conditions governing use of the identity as the “scope of permissible use,” whereas the other independent claims use the term “pre-registered condition.” The latter claims, however, specify that the pre-registered condition “defines at least one circumstance under which the identity can be used,” which corresponds to the construed meaning of “scope of permissible use.”

Claims 1, 2, and 4 of the ’456 Patent refer to “information in the request,” which “is insufficient to authorize the use of the identity.” Similarly, claim 5 of the ’456 Patent refers to “second information [that is] insufficient in and of itself to authorize any related use of the identity”; claim 1 of the ’027 Patent refers to “information [that is] insufficient in and of itself to execute the attempted use of the identity”; and claim 11 of the ’027 Patent requires that “the service provider lacks sufficient information to execute the attempted use of the identity.” The other asserted independent claims do not expressly impose a similar limitation, but, for present purposes, the Court will assume that this aspect is part of the “fundamental concept” implicitly embraced by them as well.²

² Including this limitation in all of the asserted independent claims results in an articulation more favorable to Mantissa. The more that specific features are included in the description of a claim’s

There is one notable difference between claims 1, 2, and 4 of the '456 Patent and the other asserted independent claims. The “setting,” “changing,” and “returning” steps, along with the first “wherein” clause, suggest that an important feature of the former claims is the changeable nature of the set of conditions defining the scope of permissible use. The other independent claims, by contrast, do not contain similar steps. The Court concludes that the changeability of the scope of permitted use forms part of the “basic thrust” of claims 1, 2, and 4.

To sum up, the Court, having distilled the fundamental concept embodied in the asserted independent claims, finds that their “character as a whole” can best be articulated as:

determining whether a given use of an identity is permitted based on: (i) information that is, in itself, insufficient to permit use of the identity; and (ii) a (changeable [in the case of claims 1, 2, and 4 of the '456 Patent]) set of conditions that define when the identity may or may not be used.

b. The Dependent Claims

The Court has read the forty-three asserted dependent claims in their entirety and in light of their respective specifications and concludes that they have the same “character as a whole” as the asserted independent claims upon which they depend. While the dependent claims contain additional limitations, those features are at most ancillary and do not alter the claims’ “focus” or “basic thrust” for § 101 purposes. Extended discussion of those claims is therefore unnecessary. *See Twilio, Inc. v. Telesign Corp.*, No. 16-CV-06925-LHK, 2017 WL 1374759, at *12 & n.2 (N.D. Cal. Apr. 17, 2017) (“[T]he Court need not individually analyze every claim, if certain claims are representative.”).

2. The Asserted Claims’ “Character as a Whole” Is “Directed To” an “Abstract Idea”

The Supreme Court has recognized the “longstanding rule that ‘[a]n idea of itself is not patentable.’” *Benson*, 409 U.S. at 67 (quoting *Rubber-Tip Pencil Co. v. Howard*, 87 U.S. 498,

“character as a whole,” the less likely it is that the claim will be deemed to be directed to an “abstract idea” at Step One.

507 (1874)); *see also* *Le Roy v. Tatham*, 55 U.S. 156, 175 (1852) (“A principle, in the abstract, is a fundamental truth; an original cause; a motive; these cannot be patented, as no one can claim in either of them an exclusive right.”). However, neither the Supreme Court nor the Federal Circuit has prescribed a “single, succinct, usable definition or test” for discerning a patent-ineligible “abstract idea.” *Amdocs (Israel) Ltd. v. Openet Telecom, Inc.*, 841 F.3d 1288, 1294 (Fed. Cir. 2016); *see Alice*, 134 S. Ct. at 2357 (declining to “delimit the precise contours of the ‘abstract ideas’ category in this case”); *X One, Inc. v. Uber Techs., Inc.*, No. 16-CV-06050-LHK, 2017 WL 878381, at *6 (N.D. Cal. Mar. 6, 2017) (“Neither the United States Supreme Court nor the Federal Circuit has set forth a bright line test separating abstract ideas from concepts that are sufficiently concrete so as to require no further inquiry under the first step of the *Alice* framework.”). As a result, courts conduct the “abstract idea” analysis under Step One by “compar[ing] [the] claims at issue to those claims already found to be directed to an abstract idea in previous cases.” *Enfish*, 822 F.3d at 1334; *accord Amdocs*, 841 F.3d at 1294 (“[T]he decisional mechanism courts now apply is to examine earlier cases in which a similar or parallel descriptive nature can be seen—what prior cases were about, and which way they were decided.”); *see also Alice*, 134 S. Ct. at 2357.

a. Relevant Caselaw

In *Bilski v. Kappos*, 561 U.S. 593 (2010), the Supreme Court considered the subject-matter eligibility of patent claims that described a method for hedging against the financial risk of price fluctuations. Specifically:

Claim 1 recited a series of steps for hedging risk, including: (1) initiating a series of financial transactions between providers and consumers of a commodity; (2) identifying market participants that have a counterrisk for the same commodity; and (3) initiating a series of transactions between those market participants and the commodity provider to balance the risk position of the first series of consumer transactions. Claim 4 “pu[t] the concept articulated in claim 1 into a simple

mathematical formula.” The remaining claims were drawn to examples of hedging in commodities and energy markets.

Alice, 134 S. Ct. at 2355–56 (internal citations omitted) (citing *Bilski*, 561 U.S. at 599). The Supreme Court held that the patent at issue in *Bilski* claimed “the basic concept of hedging, or protecting against risk.” 561 U.S. at 611. Finding that “[h]edging is a fundamental economic practice long prevalent in our system of commerce and taught in any introductory finance class,” the Supreme Court concluded that the claims were directed to an “abstract idea” and thus ineligible under § 101. *Id.* at 611–12 (internal quotation marks and citation omitted).

The Supreme Court next considered the “abstract idea” exception to § 101 in *Alice*. The Court described the claims at issue in *Alice* as:

relat[ing] to a computerized scheme for mitigating “settlement risk”—*i.e.*, the risk that only one party to an agreed-upon financial exchange will satisfy its obligation. In particular, the claims are designed to facilitate the exchange of financial obligations between two parties by using a computer system as a third-party intermediary. The intermediary creates “shadow” credit and debit records (*i.e.*, account ledgers) that mirror the balances in the parties' real-world accounts at “exchange institutions” (*e.g.*, banks). The intermediary updates the shadow records in real time as transactions are entered, allowing “only those transactions for which the parties' updated shadow records indicate sufficient resources to satisfy their mutual obligations.” At the end of the day, the intermediary instructs the relevant financial institutions to carry out the “permitted” transactions in accordance with the updated shadow records, thus mitigating the risk that only one party will perform the agreed-upon exchange.

In sum, the patents in suit claim (1) the foregoing method for exchanging obligations (the method claims), (2) a computer system configured to carry out the method for exchanging obligations (the system claims), and (3) a computer-readable medium containing program code for performing the method of exchanging obligations (the media claims). All of the claims are implemented using a computer; the system and media claims expressly recite a computer, and the parties have stipulated that the method claims require a computer as well.

Alice, 134 S. Ct. at 2352–53 (citations and footnote omitted). The Supreme Court held that the claims were patent-ineligible because they were “drawn to the concept of intermediated

settlement, *i.e.*, the use of a third party to mitigate settlement risk.” *Id.* at 2356. In so concluding, the Court relied heavily on *Bilski*, explaining:

Like the risk hedging in *Bilski*, the concept of intermediated settlement is “a fundamental economic practice long prevalent in our system of commerce.” [*Bilski*, 561 U.S. at 611]; see, *e.g.*, Emery, Speculation on the Stock and Produce Exchanges of the United States, in 7 Studies in History, Economics and Public Law 283, 346–356 (1896) (discussing the use of a “clearing-house” as an intermediary to reduce settlement risk). The use of a third-party intermediary (or “clearing house”) is also a building block of the modern economy. See, *e.g.*, Yadav, The Problematic Case of Clearinghouses in Complex Markets, 101 Geo. L.J. 387, 406–412 (2013); J. Hull, Risk Management and Financial Institutions 103–104 (3d ed. 2012). Thus, intermediated settlement, like hedging, is an “abstract idea” beyond the scope of § 101.

Alice, 134 S. Ct. at 2356. The Court continued:

The concept of risk hedging we identified as an abstract idea in [*Bilski*] cannot be described as a “preexisting, fundamental truth.” The patent in *Bilski* simply involved a “series of steps instructing how to hedge risk.” Although hedging is a longstanding commercial practice, it is a method of organizing human activity, not a “truth” about the natural world “that has always existed[.]” One of the claims in *Bilski* reduced hedging to a mathematical formula, but the Court did not assign any special significance to that fact, much less the sort of talismanic significance petitioner claims. Instead, the Court grounded its conclusion that all of the claims at issue were abstract ideas in the understanding that risk hedging was a “fundamental economic practice.”

In any event, we need not labor to delimit the precise contours of the “abstract ideas” category in this case. It is enough to recognize that there is no meaningful distinction between the concept of risk hedging in *Bilski* and the concept of intermediated settlement at issue here. Both are squarely within the realm of “abstract ideas” as we have used that term.

Alice, 134 S. Ct. at 2356–57 (citations omitted).

Since *Bilski* and *Alice* were decided, the Federal Circuit has “held that a wide variety of well-known and other activities constitute abstract ideas.” *Intellectual Ventures I LLC v. Symantec Corp.*, 838 F.3d 1307, 1314 & n.5 (Fed. Cir. 2016) (hereinafter, “*Symantec*”) (collecting cases). For example, it has held that patent claims “utiliz[ing] user-selected pre-set limits on spending that are stored in a database that, when reached, communicates a notification

to the user via a device” were directed to the abstract idea of “tracking financial transactions to determine whether they exceed a pre-set spending limit (i.e., budgeting).” *Intellectual Ventures I LLC v. Capital One Bank (USA)*, 792 F.3d 1363, 1367 (Fed. Cir. 2015) (hereinafter “*Capital One*”) (internal quotation marks and citation omitted).

In another case, the Federal Circuit found ineligible claims that it described as

collect[ing] information regarding accesses of a patient’s personal health information, analyz[ing] the information according to one of several rules (i.e., related to accesses in excess of a specific volume, accesses during a pre-determined time interval, or accesses by a specific user) to determine if the activity indicates improper access, and provid[ing] notification if it determines that improper access has occurred.

FairWarning IP, LLC v. Iatric Sys., Inc., 839 F.3d 1089, 1093 (Fed. Cir. 2016). In finding the claims directed to an abstract idea, the court reasoned:

We have explained that the “realm of abstract ideas” includes “collecting information, including when limited to particular content.” We have also “treated analyzing information by steps people go through in their minds, or by mathematical algorithms, without more, as essentially mental processes within the abstract-idea category.” And we have found that “merely presenting the results of abstract processes of collecting and analyzing information, without more (such as identifying a particular tool for presentation), is abstract as an ancillary part of such collection and analysis.” Here, the claims are directed to a combination of these abstract-idea categories. Specifically, the claims here are directed to collecting and analyzing information to detect misuse and notifying a user when misuse is detected.

Id. at 1093–94 (Fed. Cir. 2016) (citations omitted).

b. Application to the Asserted Claims

Defendants contend that the asserted claims “amount to no more than high-level business methods” and are “so broad” that they “cover[] routine and long-standing banking practices.” ECF No. 103 at 5–6. Mantissa maintains that the asserted claims do not encompass any “longstanding” or “fundamental” business practices and, moreover, “provide an improvement in computer network transaction processing.” ECF No. 87 at 8–9.

Identity theft and methods of preventing identity theft have existed since the dawn of civilization. *See* SANDRA K. HOFFMAN & TRACY G. MCGINLEY, *IDENTITY THEFT: A REFERENCE HANDBOOK* 1–16 (2010) (observing that “[i]dentity theft is a modern name for an ancient crime” and reviewing prominent examples of identity theft from the Book of Genesis to present times). In ancient times, identity theft generally involved “a simple form of impersonation.” *Id.* at 5. Early methods of detecting imposters and preventing such impersonation relied on correspondingly simple methods. As technology advanced and new forms of personal identification information arose, identity theft, and methods of preventing it, evolved as well. *Id.* at 6.

Two examples of longstanding practices designed to protect identity information are particularly relevant to this case. The first is found in traditional banking practices. More than a century ago, one of the key inquiries a teller at a bank was required to make before paying on a check was whether the drawer’s signature was genuine. ALBERT S. BOLLES, *PRACTICAL BANKING* 83 (8th ed. 1892). “One of the universal precautions observed by banks to prevent forgeries” was to “require every depositor to write his name in a signature book” so that the teller could compare a “doubtful” signature on a check to the appropriate signature in the book. *Id.*; *see also* *Bradford Trust Co. of Boston v. Texas Am. Bank-Houston*, 790 F.2d 407, 410–11 (5th Cir. 1986) (noting that the traditional justification for the rule that “a drawee who accepts or pays an instrument on the forged signature of the drawer is bound on his acceptance and cannot recover back his payment” is that “the drawee is in a superior position to detect a forgery because he has the maker’s signature and is expected to know and compare it”). It was recommended that “[e]very drawer should always sign his name in the same manner, or, if varying it, should acquaint the paying teller with the variation.” *PRACTICAL BANKING* 83. Similarly, when a

depositor sought to withdraw a sum of money from his account, the following process was used to determine whether the signature on the withdrawal draft was genuine:

[The paying teller] turns to the signature book (the entire series being near him), and, finding the number of the account, compares the signature of the draft held in his hand with that originally written in the book. . . . Any substantial variation, such as writing initials instead of full names, or abbreviations instead of initials, he causes to be corrected by a re-writing of the name on the back, if the depositor is present in person. . . . [The teller] must, using the best of his judgment and discretion, form his opinion as to whether the signature is genuine. . . . In the case of persons who did not write, but made a mark on the opening of their account, the mark is now made in the presence of the teller, and the person is asked the various test questions which were asked at that time. If answered correctly, and the appearance of the person sufficiently answers the description, this, with the presentation of the pass book, is considered sufficient evidence to pay on.

Id. 170–71.

The second example pertains to practices involving credit card transactions. “Although merchant credit may be as old as civilization, the present-day credit card industry in the United States originated in the nineteenth century.” Douglas Akers et al., *Overview of Recent Developments in the Credit Card Industry*, 17 FDIC BANKING REVIEW No. 3 (2005). “[B]y the early 1900s, major U.S. hotels and department stores issued paper identification cards to their most valued customers. When a customer presented such a card to a clerk at the issuing establishment, the customer’s creditworthiness and status were instantly established.” *Id.* Generally, however, these cards “were useful only at one location or within a limited geographic area—an area where local merchants accepted competitors’ cards as proof of a customer’s creditworthiness.” *Id.* By the mid-1900s, more expansive credit networks began to develop, such that by 2005, the year the ’456 Patent was filed, one commonly-used framework for credit card networks, known as the “multiple card issuer model,” involved “one card association, many cardholders, many merchants, and multiple banks.” *Id.*

In this model, the card association (or network) plays an important role by imposing rules for issuing cards, clearing and settling transactions, advertising and promoting the brand, authorizing transactions, assessing fees, and allocating revenues among transaction participants. . . . The process begins when the cardholder presents the credit card to the merchant to purchase a good or service. The merchant transmits to the acquiring bank the cardholder's account number and the amount of the transaction. The acquiring bank forwards this information to the card association network requesting authorization for the transaction. The card association forwards the authorization request to the issuing bank. The issuing bank responds with its authorization or denial through the network to the acquiring bank and then to the merchant.

Id.

As credit networks expanded in scope, methods of preventing the unauthorized use of credit cards became increasingly important and widespread. Where in-person credit card transactions are concerned, merchants have long requested additional information beyond the card itself—information like a driver's license or signature—as a means of verifying the identity of the individual attempting to use the credit card. *See Authentication in an Electronic Banking Environment*, OCC Advisory Letter, 2001 WL 897188, at *4 (July 30, 2001) (“One of the most reliable methods to verify a customer's identity is a face-to-face presentation of tangible proof of identity (e.g., driver's license).”); *Ambers v. Buy.com, Inc.*, No. 13-0196 AG JPRX, 2013 WL 1944430, at *4 (C.D. Cal. Apr. 30, 2013) (noting that, in 1991, “standard retail verification procedures” included “comparing the customer's signature to the signature on the credit card”), *aff'd*, 617 F. App'x 728 (9th Cir. 2015).

As these examples show,³ it is a longstanding, fundamental economic practice to determine whether a given use of an identity is permitted based on (i) information that is, in

³ “[I]t is well within the [c]ourt's province to make concomitant factual findings and general historical observations when making a § 101 determination.” *Network Apparel Grp.*, 154 F. Supp. 3d at 476; *accord Cal. Inst. of Tech. v. Hughes Commc'ns Inc.*, 59 F. Supp. 3d 974, 978 n.6 (C.D. Cal. 2014) (“Courts frequently make findings when deciding purely legal questions. Eligibility questions mostly involve general historical observations, the sort of findings routinely made by courts deciding legal questions.” (citations omitted)). The Supreme Court did so in *Bilski* and *Alice*, for example. *See Bilski*, 561 U.S. at

itself, insufficient to enable use of the identity, and (ii) (changeable) conditions defining when the identity may be used. In the banking example referenced above, the teller determined whether the requested transactions were permitted by comparing the signature before him (either on the check or the withdrawal draft) to the account holder's signature in the signature book. The signature in itself was insufficient to authorize the transaction. The condition defining whether the transaction was authorized was the existence of a sufficient match between the signature presented and the signature in the signature book. That condition, moreover, was changeable: the account holder could "vary" his signature (though, as the source cited above states, he would have been well-advised to inform the bank of such a change).

In the credit card example, neither a driver's license nor a signature is, in itself, sufficient to make a charge to a given credit card account. However, the merchant utilizes that "insufficient information" to determine whether use of the card is authorized by comparing it to information on the credit card itself, such as the cardholder's name and the signature on the reverse of the credit card. The condition defining the permissible use of the card is met when there is a match between the additional information (the information on the driver's license and/or the signature provided by the individual attempting to use the card) and the information on the card itself (e.g., the name on the front of the card and the signature on the reverse side). That condition, moreover, is changeable: credit card holders have long been able to add or remove other

611 (relying on general observations and financial treatises); *Alice*, 134 S. Ct. at 2356 (relying on law review articles and treatises). In other cases, the Federal Circuit has looked to whether the process at issue has an analogue in the "brick-and-mortar" context. See *Symantec*, 838 F.3d at 1317 (finding an email processing software program to be abstract through comparison to a "brick-and-mortar" post office). The Court is unaware of any authority that prevents consideration of longstanding practices, such as the banking and credit card practices noted above, in a § 101 inquiry such as this. See *Content Extraction & Transmission LLC v. Wells Fargo Bank*, 776 F.3d 1343, 1347 (Fed. Cir. 2014) (observing that "banks have, for some time, reviewed checks, recognized relevant data such as the amount, account number, and identity of account holder, and stored that information in their records").

individuals from a given account; they can also request a new card if they wish to change the appearance of their signature.

As *Bilski* and *Alice* hold, a longstanding, fundamental economic practice of this sort constitutes a patent-ineligible abstract idea. The asserted claims are also similar to the claims deemed ineligible in *FairWarning*. At their core, the asserted claims require the service provider to collect information, analyze that information in conjunction with certain conditions, make a determination based on that analysis, and notify the user of the determination. That is precisely what the claims in *FairWarning* involved. See *Fairwarning*, 839 F.3d at 1093. Indeed, the service provider is essentially a third-party intermediary, which *Alice* recognized as “a building block of the modern economy.” *Alice*, 134 S. Ct. at 2356. The Court therefore concludes that the asserted claims are analogous to “claims already found to be directed to an abstract idea in previous cases.” *Enfish*, 822 F.3d at 1334.

Mantissa contends that the asserted claims are directed to an “improvement in computer network transaction processing.” ECF No. 87 at 9. The Court finds that argument unpersuasive. “[F]undamental economic and conventional business practices are often found to be abstract ideas, even if performed on a computer.” *Enfish*, 822 F.3d at 1335. The crucial question is “whether the focus of the claims is on the specific asserted improvement in computer capabilities . . . or, instead, on a process that qualifies as an ‘abstract idea’ for which computers are invoked merely as a tool.” *Id.* at 1335–36; see also *McRO v. Bandai Namco Games Am. Inc.*, 837 F.3d 1299, 1314 (Fed. Cir. 2016) (claims “focused on a specific asserted improvement in computer animation” were non-abstract). Here, the claims simply recite, in broad, generic fashion, that the methods they describe “be[] executed on electronic computer hardware in combination with software.” Nothing in the asserted claims suggests that they are directed to improving the

functioning of computers or computer networks in and of themselves. Rather, the claims contemplate using computer networks as a tool for implementing the abstract idea identified above; any improvement to computer technology is at most incidental. *See Affinity Labs of Texas, LLC v. DIRECTV, LLC*, 838 F.3d 1253, 1262 (Fed. Cir. 2016) (claims for “providing out-of-region access to regional broadcast content” were “directed not to an improvement in cellular telephones but simply to the use of cellular telephones as tools in the aid of a process focused on an abstract idea”); *Twilio*, 2017 WL 1374759, at *16 (finding that a claim did “not improve message routing technology itself” and therefore was “not directed to an ‘improvement in computer functionality’”).

Mantissa points to what it describes as “specific limitations” in the asserted claims not comprehended by the “abstract idea” category. ECF No. 87 at 11–17. The Court finds those limitations better suited to consideration at Step Two. Although Steps One and Two of *Alice* are related and involve some overlap, *see Elec. Power Grp.*, 830 F.3d at 1353, the Supreme Court made clear in *Alice* that the two steps are distinct. At Step One, the Court must conduct “a distinct and separate inquiry . . . [by] examin[ing] the basic character of the claims as a whole in order to determine whether they are directed to an abstract idea.” *Tele-Publ’g, Inc. v. Facebook, Inc.*, No. CV 09-11686-DPW, 2017 WL 1959218, at *4 (D. Mass. May 11, 2017); *see also Tech Pharmacy Servs., LLC v. Alixa Rx LLC*, No. 4:15-CV-00766, 2017 WL 3129905, at *4 (E.D. Tex. July 24, 2017). By articulating the asserted claims’ “character as a whole” in a manner reflecting the specificity present in the claims themselves, the Court has already ensured that the Step One inquiry in this case is “meaningful.” *See Thales Visionix Inc. v. United States*, 850 F.3d 1343, 1347 (Fed. Cir. 2017).

Accordingly, the Court finds that the asserted claims are directed to an unpatentable abstract idea at Step One of *Alice*.

B. *Alice* Step Two: The Asserted Claims Do Not Contain an “Inventive Concept”

At Step Two, the Court considers “the elements of each claim both individually and ‘as an ordered combination’ to determine whether the additional elements ‘transform the nature of the claim’ into a patent-eligible application.” *Alice*, 134 S. Ct. at 2355 (quoting *Mayo*, 566 U.S. at 78–79). The Supreme Court has described Step Two as “a search for an inventive concept”—an “inventive concept” being “an element or combination of elements that is sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the ineligible concept itself.” *Id.* (internal quotation marks and brackets omitted) (quoting *Mayo*, 566 U.S. at 72–73); *accord RecogniCorp, LLC v. Nintendo Co.*, 855 F.3d 1322, 1327 (Fed. Cir. 2017).

1. Caselaw Regarding “Inventive Concept”

Like the “abstract idea” category itself, “the contours of what constitutes an inventive concept are far from precise.” *Synopsys, Inc. v. Mentor Graphics Corp.*, 839 F.3d 1138, 1151 (Fed. Cir. 2016). The Court is not without some guidance, however. It is well-established that “an inventive concept must be evident in the claims.” *RecogniCorp*, 855 F.3d at 1327; *see also Alice*, 134 S. Ct. at 2357 (“[W]e must examine the *elements of the claim* to determine whether it contains an ‘inventive concept.’”(emphasis added)); *Synopsys*, 839 F.3d at 1149 (“The § 101 inquiry must focus on the language of the [a]sserted [c]laims themselves.”). Moreover, the inventive concept “must be *significantly* more than the abstract idea itself.” *Bascom Glob. Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1349 (Fed. Cir. 2016) (emphasis added). “[A] transformation of an abstract idea to a patent-eligible application of the idea requires more than simply reciting the idea followed by ‘apply it.’” *Twilio*, 2017 WL 1374759, at

*10 (quoting *Alice*, 134 S. Ct. at 2357). The “mere recitation of concrete, tangible components is insufficient to confer patent eligibility to an otherwise abstract idea. Rather, the components must involve more than performance of ‘well-understood, routine, conventional activit[ies]’ previously known to the industry.” *In re TLI Commc’ns LLC Patent Litig.*, 823 F.3d 607, 613 (Fed. Cir. 2016) (quoting *Alice*, 134 S. Ct. at 2359). Furthermore, “limiting an abstract idea to one field of use or adding token postsolution components [does] not make the concept patentable.” *Bilski*, 561 U.S. at 612; *accord Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 709, 716 (Fed. Cir. 2014) (“Narrowing the abstract idea of using advertising as a currency to the Internet is an ‘attempt[] to limit the use’ of the abstract idea ‘to a particular technological environment,’ which is insufficient to save a claim.”); *Capital One*, 792 F.3d at 1366 (“An abstract idea does not become nonabstract by limiting the invention to a particular field of use or technological environment, such as the Internet.”).

The Federal Circuit has held that an inventive concept may be present in claims “necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks.” *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1257 (Fed. Cir. 2014). In *DDR*, the court found that claims addressed to the “Internet-centric problem” of third-party merchant advertisements “lur[ing] the [host website’s] visitor traffic away” from a host website contained an inventive concept. *Id.* at 1248, 1259. The court emphasized, however that the claims at issue did not “recite a commonplace business method aimed at processing business information, applying a known business process to the particular technological environment of the Internet, or creating or altering contractual relations using generic computer functions and conventional network operations.” *Id.* at 1259.

The Federal Circuit has also held that a “non-conventional and non-generic arrangement of known, conventional pieces” can provide an inventive concept. *Bascom*, 827 F.3d at 1350. In *Bascom*, the court concluded that a claim involving “the installation of a filtering tool at a specific location, remote from the end-users, with customizable filtering features specific to each end user” contained an inventive concept. *Id.*; *see also Amdocs*, 841 F.3d at 1301 (holding that claims “designed to solve an accounting and billing problem faced by network service providers” had an inventive concept because they contained a “specific enhancing limitation that necessarily incorporate[d] the invention’s distributed architecture”).

2. Application to the Asserted Claims

Mantissa argues that the asserted claims contain the following inventive concept:

The inventive concept in the [a]sserted [c]laims is a method with a system to effect real-time control of personal (identity) assets through use of an internet/network accessible, owner-controlled, asset state that effectively give the owner a “leash” on the asset while using “second information” or “insufficient information” similar to tokenization such that the information later cannot be used for fraudulent activity just as one would not steal a car that does not run. This is an improvement over “conventional industry practice” of using a computer network to execute financial transactions related to credit or debit cards and the remedial use of identity monitoring systems.

ECF No. 87 at 18.

The Court begins by looking at the claim limitations Mantissa identifies individually and then examines those limitations as an ordered combination. *See Bascom*, 827 F.3d at 1349 (“The ‘inventive concept’ may arise in one or more of the individual claim limitations *or* in the ordered combination of the limitations.” (emphasis added)).

a. The Individual Claim Limitations

Considered individually, none of the claim limitations provides an “inventive concept.”

i. “Real-time” Control

In their discussion of the exemplary embodiment, the specifications state that it is “helpful” for an identity owner to “be capable of modifying identification information on a whim, creating a real-time, or near real-time system that is fluid and constantly capable of meeting the needs of [the identity owner] while securing the identification information.” ECF No. 38-1 at 5:53–58. However, the asserted claims themselves do not refer to “real-time” control. Furthermore, the asserted claims do not “include any requirement for performing the claimed functions . . . in real time by use of anything but entirely conventional, generic technology.” *Elec. Power Grp.*, 830 F.3d at 1356. Instead, the asserted claims contemplate “real-time” control solely as the result of the ordinary functioning of computer networks, which is insufficient to supply an inventive concept. *See Capital One*, 792 F.3d at 1370 (“[O]ur precedent is clear that merely adding computer functionality to increase the speed or efficiency of the process does not confer patent eligibility on an otherwise abstract idea. . . . [T]he fact that the web site returns the pre-designed ad more quickly than a newspaper could send the user a location-specific advertisement insert does not confer patent eligibility.”).

ii. Internet/Network Accessibility

The mere fact that the identity asset state is accessible via internet or computer network is plainly insufficient to establish an inventive concept. *See Mortg. Grader, Inc. v. First Choice Loan Servs. Inc.*, 811 F.3d 1314, 1324–25 (Fed. Cir. 2016) (holding that “generic computer components such as an ‘interface,’ ‘network,’ and ‘database’ . . . do not satisfy the inventive concept requirement.”); *Bancorp Servs., L.L.C. v. Sun Life Assur. Co. of Canada (U.S.)*, 687 F.3d 1266, 1278 (Fed. Cir. 2012) (“To salvage an otherwise patent-ineligible process, a computer

must be integral to the claimed invention, facilitating the process in a way that a person making calculations or computations could not.”).

iii. Owner Control

None of the asserted claims states that the identity owner has untrammelled control over the identity asset state. In fact, some asserted claims, such as claim 11 of the '456 Patent, specify that the user, not the identity owner, establishes the “set of desired identification information parameters.” While the identity owner can then supply information consistent with those parameters, the fact that the user exercises significant control over the asset state undercuts any notion that the asserted claims contain an “inventive concept” founded on “owner control.” Indeed, the control reserved to a user under those claims is not unlike the control credit card companies have long exercised over cardholders’ ability to craft conditions governing use of their accounts. In any event, the mere idea of permitting an identity owner (rather than the user) to set the conditions under which his or her own identity can be used is not, without more, an inventive concept.

iv. The Proactive “Leash”

Mantissa distinguishes the purportedly “proactive” or “leash”-like nature of the asserted claims from the “remedial” orientation of “conventional industry practice.” The declaration of Gary M. Dennis, one of the co-inventors of the patents-in-suit, provides further explanation:

The conventional focus was on the credit card company’s ability to control the identity information, not the unconventional and novel approach where an owner of the identity applies a “leash” to the use of his or her own identity assets. For example, in [c]laim 1 [of the '456 Patent] the “leash” is applied by “defining a scope of permitted use of the identity; changing . . . status to a second state defining a scope of permitted use of the identity that is different from the first state” where the “information in the request is insufficient to authorize.” Other claims express the “leash” in terms of “pre-registered conditions” set by the identity owner. *See e.g.* '456 Patent, Claim 11, 14, 15. This focus is even a departure today from the identity protection services such as Life Lock® or Free

Credit Report.com® that reactively notify if identity information (sufficient to authorize a transaction) is used. Remediation in all cases is more problematic and costly than prevention.

ECF No. 102-1 at ¶ 30.

With the exception of claim 14 of the '456 Patent and claim 10 of the '027 Patent, none of the asserted claims prevents *both* (i) the user from authorizing a use of the entity's identity absent permission from the service provider *and* (ii) the service provider from providing permission unless consistent with "the intent of the entity." Without those limitations, the user could authorize a use of the identity that the service provider did not determine was permitted, or the service provider could provide permission even if doing so was not consistent with the information and conditions before it. In either case, the "scope of permitted use" or "pre-registered conditions" would not be acting as a proactive leash over use of the identity. As noted above, an "inventive concept" must appear in the claims themselves. Thus, with two exceptions, none of the asserted claims even arguably has the inventive proactive nature Mantissa ascribes to them.

Looking to claim 14 of the '456 Patent and claim 10 of the '027 Patent, the Court finds that a proactive leash is not an inventive concept with respect to either claim. Mr. Dennis maintains that it "was a new technology in 2005 for an identity owner in a computer or communication network to proactively control use of identity and identification information by applying a 'leash' to his or her information where the information can be used but is without value to an outside intruder." ECF No. 102-1 at ¶ 32. Taking that assertion as true for present purposes, it nonetheless remains the case that requiring a given use of an identity to be consistent with certain conditions set down in advance is an abstract idea. Applying that idea to computer networks may have been new in 2005, but "[a]n abstract idea does not become nonabstract by

limiting the invention to a particular field of use or technological environment.” *Capital One*, 792 F.3d at 1366.

v. Use of “Second Information”/“Insufficient Information”

This limitation was included as part of the Court’s articulation of the asserted claims’ “character as a whole.” Insofar as Mantissa repeats the arguments already considered at Step One, the Court rejects those arguments for the same reasons given before.

Mantissa suggests that the use of second/insufficient information exemplifies the asserted claims’ inventive “layered” structure, which it describes as

limiting the exposure of the identity assets by consummating a transaction with a layered approach using only insufficient identity information known to only limited and specified participants in the transaction, . . . preventing hacking at the participant respective sites because, by analogy, a thief won’t steal a car that doesn’t run, and . . . significantly reducing the computing, data storage, necessary bandwidth, and archival requirements with the [a]sserted [c]laims’ “layered” approach to prevent transaction fraud.

ECF No. 87 at 11.

None of the asserted claims recite a layered structure that precludes *both* the user *and* the service provider from having all the information necessary to authorize a use of the identity. For example, in claim 5 of the ’456 Patent, “first information” is forwarded to the user, and the user forwards “second information” to the service provider. The user therefore has access to both the first and second information. Nor is there any limitation stating that the user does not have access to the “pre-registered condition(s).” If the user is hacked, all of this information is presumably vulnerable. In claim 11 of the ’456 Patent, the entity provides certain information directly to the service provider, and the service provider also responds to a request by the user to authorize the transaction. The user “does not have direct access to the information provided by the entity” to the service provider. ECF No. 38-1 at 16:57–58. But unlike other claims in the ’456 Patent, claim

11 does not impose any limitations on the information in the request to the service provider. Thus, under claim 11, the service provider may well have access to information sufficient to authorize a use of the identity, thus exposing such information to hacking at a single site.

The specification confirms this. The discussion of the exemplary embodiment states that the information in the request from the user to the service provider “is *preferably* in and of itself insufficient to enable the use of the identity for its intended use, such that its capture or loss would not expose vital information.” ECF No. 38-1 at 4:58–61 (emphasis added). It also states that it is preferable that the service provider “authorizes or denies requests without having access to sensitive identification information, . . . [and] does not have enough information to take any action on its own.” ECF No. 38-1 at 6:54–59. But the specification expressly acknowledges that “[i]n theory,” the service provider “may nonetheless have access to some of this information, although such information can be protected using passwords, encryption, or other known techniques.” ECF No. 38-1 at 6:64–67. The claims themselves, however, do not recite any such protective technique.

To the extent that *either* the user *or* the service provider does not have access to information sufficient to authorize use of the identity, the “layered” structure arguably provides *some* benefit in terms of identity protection. But the Court is not persuaded that this supplies “*significantly* more” to the underlying abstract idea. This feature is more akin to claim limitations that merely involve “manipulating, reorganizing, or collecting data” as opposed to “fundamentally altering the original confidential information.” *Card Verification Sols., LLC v. Citigroup Inc.*, No. 13 C 6339, 2014 WL 4922524, at *5 (N.D. Ill. Sept. 29, 2014).

Finally, any “inventive concept” relating to the “layered” approach in terms of data storage, bandwidth, and archival requirements is not evident in the claims themselves. Limiting

the information provided to transaction participants may well result in the benefits Mantissa references, but without more, it does not add anything significant to the abstract idea.

b. The Limitations Considered as an Ordered Combination

Considering them as an ordered combination, the Court concludes that the purported claim limitations identified above do not add an inventive concept sufficient to render the asserted claims patent-eligible.

The asserted claims are not “necessarily rooted” in computer technology in order to overcome a problem specifically arising in the realm of computer networks. *See DDR*, 773 F.3d at 1257. Hacking identification information may be a problem limited to computer networks, but identity theft is not. It is the latter problem that the claims address, and the solution they provide is decidedly technology-independent. The asserted claims do not require doing something *to* computer networks, they require doing something *with* computer networks. *See DIRECTV*, 838 F.3d at 1262 (explaining that *DDR* “dealt with a patent that required doing something *to* a web page, not simply doing something *on* a web page, a difference that the court regarded as important to the issue of patent eligibility”).

Nor does the ordered combination of elements in the asserted claims recite a “non-conventional and non-generic arrangement of known, conventional pieces.” *See Bascom*, 827 F.3d at 1350. As explained above, none of the individual limitations is unconventional, and the Court finds nothing in the combination of those elements that is, either.

Based on the foregoing, the Court concludes that the asserted claims fail to recite an inventive concept under Step Two.

C. There Are No Genuine Issues of Material Fact

Mantissa cites evidence from various sources to support its assertion that triable issues of fact exist at Step One and/or Step Two of *Alice*. None of that evidence is availing.

Mantissa relies heavily on Gary Dennis’ declaration. *See* ECF No. 102 at 5–8. The Court has already considered, and rejected, some of the assertions Mr. Dennis makes concerning the asserted claims’ purported inventiveness. Beyond that, it bears mentioning that “[t]he ‘novelty’ of any element or steps in a process, or even of the process itself, is of no relevance in determining whether the subject matter of a claim falls within the § 101 categories of possibly patentable subject matter.” *Diamond v. Diehr*, 450 U.S. 175, 189 (1981). More generally, the fact that Mr. Dennis’ testimony reaches legal conclusions contrary to the Court’s is irrelevant for summary judgment purposes; legal conclusions are the sole province of the Court. *See Mortg. Grader*, 811 F.3d at 1325–26 (finding that expert’s declaration did not preclude summary judgment under § 101); *ICON Health & Fitness, Inc. v. Polar Electro Oy*, No. 1:11-CV-00167-BSJ, 2017 WL 978993, at *10 (D. Utah Mar. 10, 2017).

Mantissa also cites a 2016 press release from Ondot and articles published between 2014 and 2015 in three periodicals—*Network World*, *BanklessTimes*, and *TechCrunch*—describing Ondot’s allegedly infringing product and characterizing it as an improvement over existing technology. ECF No. 102 at 13–15. Given the timing of these publications (nine years or more after the ’456 Patent was filed) and the fact that they deal with Ondot’s product, rather than Mantissa’s, the Court finds that they do not create a genuine issue of material fact.

D. Preemption

The underlying concern that drives the implied exclusions to subject-matter eligibility under § 101 is “one of pre-emption.” *Alice*, 134 S. Ct. at 2354. Laws of nature, natural

phenomena, and abstract ideas constitute “‘the basic tools of scientific and technological work.’” *Id.* (quoting *Myriad Genetics*, 133 S. Ct. at 2116). Allowing such “building blocks of human ingenuity” to be monopolized “‘through the grant of a patent might tend to impede [i.e., preempt] innovation more than it would tend to promote it,’ thereby thwarting the primary object of the patent laws.” *Alice*, 134 S. Ct. at 2354 (quoting *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 71 (2012)).

Mantissa argues that the asserted claims “do not risk preempting all future inventions for these types of computer network transactions.” ECF No. 85 at 24. At the very least, Mantissa contends, there is a material fact issue as to whether the asserted claims would preempt innovation. These arguments are unavailing. “While preemption may signal patent ineligible subject matter, the absence of complete preemption does not demonstrate patent eligibility.” *Synopsys, Inc. v. Mentor Graphics Corp.*, 839 F.3d 1138, 1150 (Fed. Cir. 2016) (internal quotation marks omitted) (quoting *Ariosa Diagnostics, Inc. v. Sequenom, Inc.*, 788 F.3d 1371, 1379 (Fed. Cir. 2015)); *accord Cleveland Clinic Found. v. True Health Diagnostics LLC*, 859 F.3d 1352, 1363 (Fed. Cir. 2017); *FairWarning*, 839 F.3d at 1098. “Where a patent’s claims are deemed only to disclose patent ineligible subject matter under the [*Alice*] framework”—as the Court deems the asserted claims in this case—“preemption concerns are fully addressed and made moot.” *Id.* Accordingly, any factual issue regarding the preemptive impact of the patents-in-suit is immaterial and does not preclude summary judgment in Defendants’ favor.

E. Defendants’ Motion for Judicial Notice

As noted above, Defendants request that the Court take judicial notice of a 1995 American Bar Association article concerning living trusts. They maintain that the article shows

that living trusts are a “well-known business method” and therefore supports finding that the asserted claims do not contain an “inventive concept.” ECF No. 80 at 8.

The Court concludes that the subject matter of the article is not reasonably analogous to the patents-in-suit and would not be probative with respect to patent eligibility under § 101. *See Dawes v. Imperial Sugar Co.*, No. 4:11-cv-3250, 2013 WL 1345635, at *2 (S.D. Tex. Mar. 30, 2013) (Rosenthal, J.); *U.S. ex rel. Modglin v. DJO Glob. Inc.*, 48 F. Supp. 3d 1362, 1383 (C.D. Cal. 2014) (declining to take judicial notice of documents that were “not probative”), *aff’d*, 678 F. App’x 594 (9th Cir. 2017). In any event, the Court has already determined that Defendants are entitled to summary judgment, and considering the article will not alter that conclusion. The renewed motion for judicial notice is therefore denied as moot.

F. Defendants’ Motion to Strike

When the Court notified the parties of its decision to convert Defendants’ motion for judgment on the pleadings into a motion for summary judgment, it set two deadlines: a June 9, 2017 deadline for the parties to file “any additional briefing,” and a June 16, 2017 deadline for any party to file “a response” to an opposing party’s “additional briefing.” Mantissa filed additional briefing in accordance with the June 9 deadline, but Defendants did not. However, Defendants filed a response to Mantissa’s additional briefing on June 16. On June 23, Mantissa filed a reply to Defendants’ response, as well as a declaration of Sandeep Chatterjee, Ph.D., a technical expert whom Mantissa has retained. ECF Nos. 105, 106.

Defendants move to strike the reply and declaration as unauthorized by the Court’s briefing order. ECF No. 107. Rule 12(d) requires that, following conversion, “[a]ll parties must be given a reasonable opportunity to present all the material that is pertinent to the motion.” FED. R. CIV. P. 12(d). Mantissa’s only opportunity to respond to arguments made by Defendants after

conversion to summary judgment was by filing the instant reply and declaration. Given that, and because Mantissa is the non-moving party, the Court denies the motion to strike. Defendants' request that they be permitted to file a sur-reply is denied.

Having considered the additional arguments in Mantissa's reply, the Court remains of the opinion that Defendants are entitled to summary judgment. Many of his statements, especially those concerning industry practices, are highly equivocal. *See, e.g.*, ECF No. 106 ¶ 40 ("I do not believe this was conventional in 2005."). Moreover, his statements are directed toward legal conclusions rather than material fact issues. The Court therefore finds that Dr. Chatterjee's declaration fails to create a genuine issue of material fact.

IV. CONCLUSION

For the reasons given above, the Court concludes that the asserted claims of the patents-in-suit are not eligible for patent protection under § 101. This does not mean that the methods described in the patents have not advanced identity protection. Under current law, however, "[g]roundbreaking, innovative, or even brilliant discovery does not by itself satisfy the § 101 inquiry." *Ass'n for Molecular Pathology v. Myriad Genetics, Inc.*, 133 S. Ct. 2107, 2110 (2013).

The Court therefore **GRANTS** summary judgment in favor of Defendants. In addition, the Court **DENIES as moot** Defendants' renewed motion for judicial notice and **DENIES** Defendants' motion to strike. A separate order of dismissal will follow.

Signed on August 10, 2017, at Houston, Texas.



DENA HANOVICE PALERMO
UNITED STATES MAGISTRATE JUDGE